

Chapter 20



Reports

NetVigil has extensive and flexible reporting at various levels (container, device, tests) as well as of different types (fault, performance, SLA). Most reports are generated in real-time by collecting data from the DGEs and then creating the graphs and statistics from the raw data by the BVE reporting engine.

There are three levels of reports with increasing levels of flexibility: Summary, Advanced and Custom. The reporting framework is very flexible and allows completely arbitrary custom reports and statistics generated on the fly.

The different types of reports available from NetVigil are:

- **Fault Management Reports:** Includes Event History, Service Instability report, Device Instability, Threshold Violations
- **Performance and Capacity Planning:** Top N usage and trend report, 30 Day upcoming trends
- **SLA Reports:** Unavailability, Downtime
- **Alarm Reports:** derived from traps or syslog messages
- **Stored/Scheduled Reports:** Modify, Execute or delete queries

The graphs can scale to normal or logarithmic, and you can zoom into the different graphs or export the data in CSV format.

20.1 Summary Reports

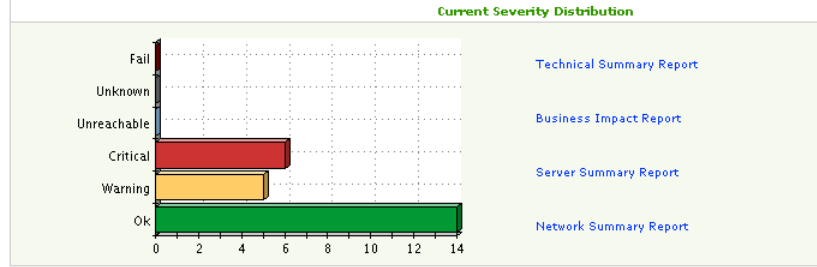
These reports give a quick snapshot for the past week. There are reports for a technical manager, and executive reports for a business manager showing the impact on business service containers.



STATUS REPORTS

summary advanced custom logout

Summary Report



[Technical Summary Report](#)

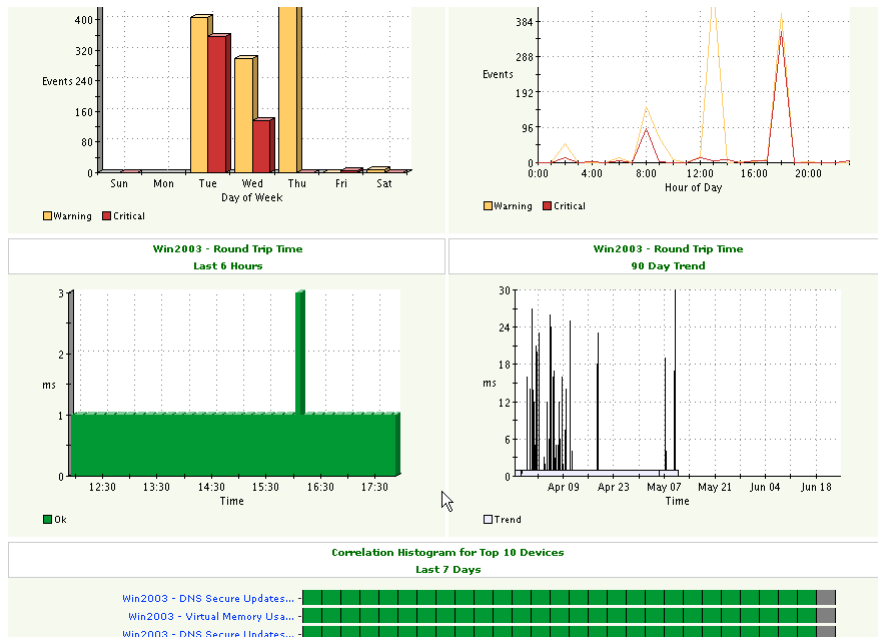
[Business Impact Report](#)

[Server Summary Report](#)

[Network Summary Report](#)

20.1.1 Technical Summary Report

This report gives the top N problems, distribution of problems by day of week, correlation graphs for all devices that had problems over the past week, trend graphs for various elements, network, CPU and disk issues over all devices.




20.1.2 Business Impact Summary

This report shows which devices or elements caused various service containers to go down, correlation graph for the top 10 service containers (excluding OK elements), top N service containers sorted by downtime. All reports are interactive, so you can drill down further into any report for much more detailed analysis in real-time.

Business Impact Report
5/3/05 - 5/10/05

Top 10 business service impacts - Last 7 days					
Test	Device	# Events (Warn/Crit)	Total Downtime (Warn/Crit)	Services Impacted	
Oracle Table (oradb9.fidelia.com: SYSTEM) Space Util	Oracle Server	0 / 1	00h 00m / 7d 00h 00m	eCommerce Service Ecomm Cont. KDM container 2	
Oracle Table (oradb9.fidelia.com: XDB) Space Util	Oracle Server	0 / 1	00h 00m / 7d 00h 00m	KDM container 2 eCommerce Service Ecomm Cont.	
Oracle Table (oradb9.fidelia.com: EXAMPLE) Space Util	Oracle Server	0 / 1	00h 00m / 7d 00h 00m	eCommerce Service Payroll Service Ecomm Cont. KDM container 2	
Disk C: (System) Space Util	winserv		5m / 00h 00m	eCommerce Service	
GigabitEthernetTP25, Traffic Out	Dell Switch	13 / 0	6d 21h 26m / 00h 00m	KDM container 2 Finacial Risk Mgt eCommerce Service Payroll Service Network	



NetVigil Progress

Gathering performance data from DGEs...

Figure 20.1 Top-N service container outages

Event Correlation Chart

The Event Correlation chart is generated in a number of different reports. This chart shows a 24 hour snapshot of all the individual elements of a service container or a device. If a particular test has gone into any non-OK state within an hour, that hour is colored to reflect the non-OK state. This report allows you to correlate various problems in your service container or device and see what events happened during the same hour during the day.

20.2 Advanced Reports

These reports give operational and engineering analysis of your IT infrastructure and answer some commonly asked questions.

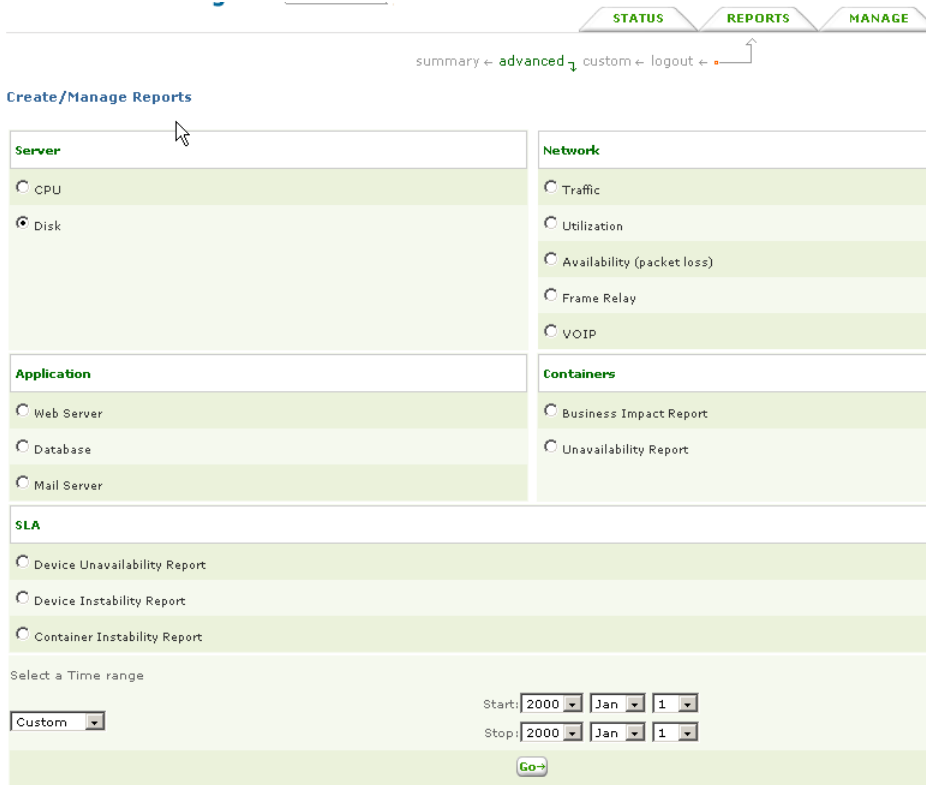


Figure 20.2 Advanced Reports Menu

20.2.1 Fault Management Reports

The Fault Management Reports provide an in-depth and rigorous analysis of the events where tests/devices and services crossed the thresholds. They provide Device and Service reports on the most fault prone services and the number of events that occurred.

These reports use events (or threshold violations) to calculate the number of times or the total time spent in warning or critical conditions. These reports answer questions such as:

- Availability: what was the total time for which monitored elements were unavailable?
- How many outages occurred?
- What was the average time of an outage (MTTR)?

Event History is designed to provide a consolidated view of events for either the last 24 hours or for a specific historical month. Each report entry is a unique combination of device name, test name and severity, detailing both the total duration in the specified severity (i.e. CRITICAL, WARNING, etc.) and the number of times that the test entered that severity. Below the text listing is a graphical display of the top 10 'worst' results in a horizontal bar style. Clicking on any of the column headings for the text list will automatically update this graph.

Service Instability provides reports on top 10, 25 or 50 services affected by number of events. The report consists of the Frequency distribution of the events during each hour of the day, each day of the week/month and duration of events.

Device Instability provides reports on top 10, 25 or 50 services affected by number of events. The report consists of the Frequency distribution of the events during each hour of the day, each day of the week/month and duration of events. You can choose all or a category of devices.

Threshold Violation Reports provide you with data on threshold violations for Bandwidth, CPU, Memory and Disk Utilization.

20.2.2 Performance and Capacity Planning Reports

These reports help you plan managing your IT infrastructure investments and targeting them in right direction. These reports help to know where exactly the performance is the bottleneck due to capacity constraints.

Top 'N' Usage & Trend Report gives useful data on the capacity planning for creating redundant capacity where required and removal of excess capacity where it is not required by reporting on TOP N devices or Tests by highest or lowest usage values. This report can be based on the status of one or more test types.

30 Day Upcoming Trends for Bandwidth, CPU and Disk Space utilization gives a trend analysis for next one month and allows you to plan accordingly.

20.2.3 SLA Reports

Unavailability/Downtime Report The Unavailability/Downtime SLA Report is based on device availability as measured by the ICMP packet loss test. The report shows how many times and for how long Packet Loss tests were in the Critical or Unreachable states. The SLA threshold for the Packet Loss test is used to determine when the test was in Critical state. This report shows the Top 10 devices by amount of “unavailability”, displaying total time unavailable and %-unavailable, with graphics showing either view.

Users may link to an availability distribution report/graph as well. This histogram is a distribution of the numbers of devices falling into blocks of 10% availability. That is, it displays the number of devices falling between 0-10% availability, 10-20% availability, and so on.

Threshold Violation Report The Threshold Violation report allows you to run reports on system resources (CPU, disk space, bandwidth, etc.), comparing test results with SLA thresholds.

You can also create custom reports for other tests using SLA thresholds.

❑ To create custom reports that use SLA thresholds:

1. Click `REPORTS` | `Custom`.
2. On the Create Test Level Report page, set the **Severity** field to `SLA`.
3. Select other report parameters, and then click **GO**.

20.2.4 Alarm Reports

For alarms generated from text messages such as SNMP traps, syslog messages or other logs inserted via the ISM API, the following reports are available:

- Top N alarms
- Top N alarms by frequency
- Alarm count by time of day

20.3 Custom Reports

In addition to the large number of preset reports listed above, NetVigil offers complete flexibility in creating ad-hoc reports over any time period. You can select the data over which to generate the report by specifying the device or test names, the time period and other such parameters. You can decide on the type of report to be generated such as a top-N table, or a trend report, a correlation graph, etc.

The categories available under Custom reports are:

Fault Level Reports Generates one or more of the Top Ten, Number of Events Distribution, Event Duration Distribution, Number of Events, for the particular tests of chosen test types for a device.

Performance Generates reports for capacity planning, trend analysis, statistical analysis, etc.

Inventory Reports Shows the distribution of your IT infrastructure by vendor type, OS, etc.

20.4 Stored and Scheduled Reports

You can save any custom or advanced report and then schedule the report to be run automatically and email the results if desired. Whenever an advanced or custom report is generated, a 'Save' option is displayed on the report to save it under a custom name. These saved reports are all listed under this menu item.

logged in as widget_ny (user)

STATUS REPORTS MANAGE HELP

summary ← advanced custom ← logout ←

Create Scheduled Report
Select or complete the required fields below. Click 'Create Scheduled Report' to confirm.
* - indicates a required field

* Scheduled Report Name : Scheduled Report

Temporarily Suspend This Report :

* Generate Using Saved Query : Bandwidth Report

* Email Generated Report to : address from current user's profile
 following address(es)
victor.mooney@fidelia.com
robert.wiley@fidelia.com
specify one address on each line

* Report Should Be Sent : One Time Only
 Every 1 Week(s)

* Starting With : May 10 2005

Create Scheduled Report Reset

Depending on the schedule selected, reports are emailed at following times:

schedule	report mailed at
daily	12.00 am
weekly	12.00 am, every monday
monthly	12.00 am, last day of the month

The time is dictated by the time-zone of the NetVigil host. At 12:00am, each scheduled job is processed sequentially and sent via email to the address specified in the user's preference. If there are multiple jobs scheduled for the same time, the actual time when the email is sent will depend on how long the jobs ahead in the queue takes to complete.

The reports are sent via the email server configured in etc/netvigil.xml. If there are multiple email servers configured, if the first email server is non-responsive, the next server will be used and so on.

